*УДК 004*

# ПОДХОДЫ К РАСПРЕДЕЛЕНИЮ КЛЮЧЕВОЙ ИНФОРМАЦИИ

**Абеева К.И., Новиков Д.И., студенты 4 курса**
**Научный руководитель – Субаева А.К.,**
**доктор экономических наук, доцент**
**Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ Чистопольский филиал «ВОСТОК»**

***Ключевые слова:*** *Передача данных, хранение данных, безопасность, ключевая информация, сеть, доступ, данные.*

*В статье рассматриваются подходы к распределению ключевой информации. В сфере информатики, изучающей передачу и хранение данных, информация занимает центральное место в современном обществе. Разнообразные методы, такие как использование криптографических сетей и иерархических структур ключей, способствуют эффективному управлению ключевой информацией. Хотя случайное распределение ключей может снизить вероятность утраты информации, необходимо уделить особое внимание контролю доступа к ключам. Гарантировать надежность и безопасность обмена данными в сети является важным для защиты информации от несанкционированного доступа.*

Передача и хранение данных – это сфера информатики, которая исследует способы распределения и сохранения информации, учитывая вероятность различных событий. В первую очередь, информация связана с социальным взаимодействием людей, но она так же присутствует и в других живых существах, а также в различных технических устройствах.

Информация стала ключевым ресурсом современного мира, выступая в качестве объекта отношений, цели действий, средства и условия для достижения результата, а также товара, который имеет свою стоимость в реальном и концептуальном смысле. «Информация»–

одна из основных категорий современных явлений, включая процесс познания. Тем не менее, она является неоднозначной и не имеет точных границ и определений в научной сфере. Основы научного исследования информации были заложены в работах Н.Винера, У.Р.Эшби и К.Э.Шеннона [1].

Параметры, определяющие основную структуру:

-время, необходимое для передачи основного компонента (ключей);

-количество передаваемой основной информации;

-необходимый объем памяти для хранения основной информации;

-устойчивость основной структуры к различным видам угроз[1].

**Таблица 1. Виды ключевых структур**

| Тип | Объем КИ на 1 узел | Объем КИ в сети | Устойчивость |
|---|---|---|---|
| Единичный | n | nM | Низкая |
| Сетевой | n(M-1) | nM(M-1) | Высокая |
| Базовый | nL | nML | Требуемая |

Описать использование блокчейна в агропромышленности: "Блокчейн-технология, упомянутая в таблице 1, находит все большее применение в агропромышленности. Например, блокчейн может использоваться для отслеживания происхождения продуктов питания, гарантируя их качество и безопасность. Также блокчейн может применяться для автоматизации финансовых операций, связанных с сельскохозяйственным производством и торговлей.

На сегодняшний день для распределения открытых ключей применяются следующие требования: открытый ключ должен соответствовать закрытому ключу;секретность ключа не является обязательной; целостность ключа должна быть обеспечена; владелец ключа должен быть аутентифицирован[2].

Ключевая информация является основой безопасности любой криптографической системы. Важным аспектом распределения ключевой информации является обеспечение достаточной защиты, чтобы предотвратить несанкционированный доступ к данным, а также гарантировать надежность и безопасность обмена данными между различными участниками сети.Существуют различные подходы к

распределению ключевой информации, используемые в современных криптографических системах.

В этом подходе ключи генерируются и хранятся на разных серверах по всему миру. Это уменьшает риск потери ключевой информации при атаке на одну из серверов, а ключи могут генерироваться случайным образом или с использованием криптографических алгоритмов[3].

**Таблица 2. Основные технологии управлении ключами**

| Название технологий | Определение |
|---|---|
| Блокчейн | технология, которая позволяет хранить и распространять данные в децентрализованной сети. В подходе случайного распределения ключей с использованием блокчейна, ключи хранятся в блокчейне, и доступ к ним осуществляется через криптографические алгоритмы. Это может обеспечить дополнительную защиту от несанкционированного доступа к данным и упростить процесс распределения ключей между участниками сети. |
| Криптографические алгоритмы | для распределения ключей могут использоваться для генерации, распространения и хранения ключей. Например, алгоритмы с открытым ключом, такие как RSA, позволяют генерировать пару ключей – открытыйи закрытый. Открытый ключ может быть распространен между участниками сети, а закрытый ключ используется для декриптования данных. Это может упростить процесс распределения ключей и обеспечить надежность и безопасность обмена данными. |
| Хэширование | процесс преобразования данных в уникальный код, который может использоваться для проверки данных на точность и безопасность. В подходе к распределению ключевой информации с использованием ключевых слов и хэширования, ключи могут быть преобразованы в хэш-коды и храниться вместе с ключевыми словами. Это может обеспечить дополнительную защиту от несанкционированного доступа к ключам и упростить процесс их распределения и управления. |
| Ключевые контейнеры | специальные файлы или приложения, которые могут хранить и защищать ключи от несанкционированного доступа. В подходе к распределению ключевой информации с использованием ключевых контейнеров и хранения ключей на серверах, ключи могут быть храниться на серверах, которые находятся в разных географических регионах. Это может уменьшить риск потери ключевой информации при атаке на одну из серверов и обеспечить надежность и безопасность обмена данными. |

Криптографические сети – этосети из нескольких узлов, работающих вместе для генерации, хранения и распространения ключей. Каждый узел в сети имеет свою роль и отвечает за определенные аспекты процесса распределения ключей. Криптографические сети могут обеспечивать дополнительную защиту от атак и обеспечивать надежность и безопасность обмена данными.

В иерархической структуре ключей ключи организованы в иерархию уровней, где каждый уровень имеет свой ключ, используемый для зашифровки ключей на более низких уровнях. Это позволяет разделить ответственность за хранение и управление ключами между различными участниками сети [4].

Бинарное дерево ключей – этоиерархическая структура ключей, в которой каждый узел представляет собой ключ, и у каждого узла есть два потомка, используемых для зашифровки и расшифровки данных. Это позволяет создавать сложные иерархические структуры ключей, обеспечивающие дополнительную защиту и гибкость в распределении ключевой информации [5].

В подходе случайного распределения ключей, ключи распределяются случайным образом между участниками сети, что может уменьшить риск потери ключевой информации. Однако, этот подход может привести к сложностям в управлении ключами и доступом к ним, а также может быть неэффективным при большом количестве участников сети [6].

Таким образом, можно сделать вывод о том, что распределение ключевой информации является важным аспектом современных криптографических систем и подчеркивает важность выбора подходящей стратегии для распределения ключевой информации в зависимости от потребностей. Для эффективного распределения ключевой информации необходимо учитывать особенности организации, требования к безопасности и конфиденциальности, а также возможности и ограничения используемых технологий.Результаты исследования могут быть полезны для специалистов в области информационной безопасности, а также для организаций, которые стремятся обеспечить надёжную защиту своих данных.

**Библиографический список:**

1. Передача, хранение и обработка информации [Электронный ресурс]. – Режим доступа: https://elar.urfu.ru

2. Защита компьютерной информации [Электронный ресурс]. – Режим доступа:https://library.voenmeh.ru

3. Информационная безопасность в интернете [Электронный ресурс]. – Режим доступа: https://www.jetinfo.ru

4. Защита информации компьютерных систем[Электронный ресурс]. – Режимдоступа: https://www.sviaz-expo.ru

5. Бинарное дерево [Электронный ресурс]. – Режим доступа:https://dev-gang.ru

6. Технология блокчейн с точки зрения ИБ [Электронный ресурс]. – Режим доступа: https://safe-surf.ru

## APPROACHES TO THE DISTRIBUTION OF KEY INFORMATION

**Abeeva K.I., Novikov D.I.**
**Scientific supervisor – Subaeva A.K.**
**Kazan National Research Technical University named after A.N. Tupolev – KAI EAST Chistopol branch**

***Keywords:*** *Data transmission, data storage, security, key information, network, access, data.*

*The article discusses approaches to the distribution of key information. In the field of computer science, which studies data transmission and storage, information occupies a central place in modern society. A variety of methods, such as the use of cryptographic networks and hierarchical key structures, contribute to the effective management of key information. Although random key allocation can reduce the likelihood of information loss, special attention should be paid to key access control. Ensuring the reliability and security of data exchange on the network is important to protect information from unauthorized access.*